Microsoft

TechNet UC

Fix Misconfigurations. Fortify Your Intune

Intune Remediation

Engagement Results

- Fully remediated Intune environment, aligned with Microsoft best practices
- Enhanced protection against device threats and unauthorized access
- Reduced risk of data leakage and endpoint-based attacks
- Improved compliance with regulatory and organizational standards

"In today's fast-paced digital landscape, where organizations rely heavily on technology to drive their operations, effective configuration management is a cornerstone of success."

Is your organization's device management environment truly protected against evolving threats, or could misconfigurations in Intune be silently exposing your business to risk?

The Foundation of Secure Device Management

Microsoft Intune is the cornerstone of modern endpoint management. Misconfigurations and outdated policies can lead to vulnerabilities, compliance issues, and operational inefficiencies. TechNet UC's Intune remediation ensures your environment aligns with Microsoft's Zero Trust principles, security frameworks, and operational best practices.

By proactively remediating your environment, you'll strengthen your organization's resilience and ensure devices remain secure, compliant, and productive.

Why Remediate Your Intune Environment

A misconfigured Intune environment can quietly expose your organization to security threats, compliance gaps, and operational inefficiencies. Remediation ensures your device management infrastructure is aligned with Microsoft's best practices—strengthening protection, simplifying management, and supporting regulatory readiness.

Review your current Intune configuration and security posture

Recalibrate device compliance, configuration, and application policies

Implement Conditional Access, endpoint protection, and data loss prevention

Configure role-based access controls and audit logging to keep your environment secure

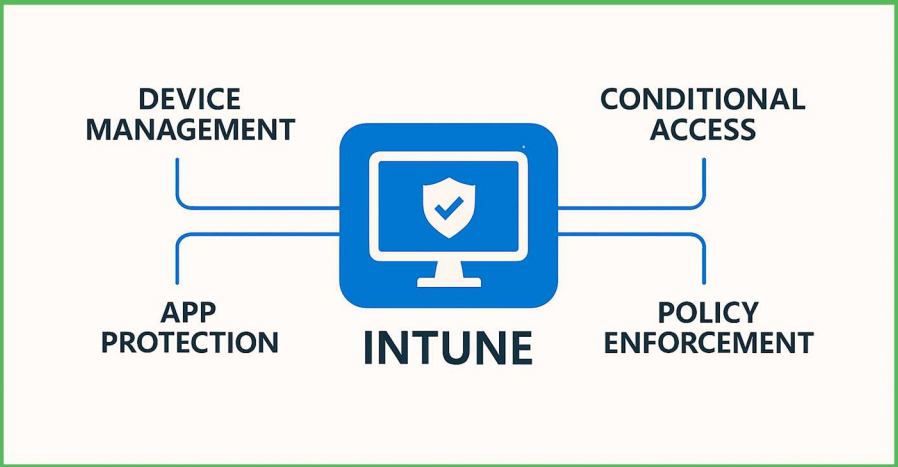
What to expect

TechNet UC's certified experts will assess your Intune configuration, security posture, and compliance settings. We'll remediate device compliance and configuration policies, implement Conditional Access and endpoint protection, and integrate with Microsoft Defender for Endpoint and Entra ID.

We'll work with you to:

- Review your current Intune configuration to identify gaps and risks
- Implement recommended security and compliance controls
- Configure Conditional Access, DLP, and app protection policies for compliance and protection
- Deliver documentation of changes, operational guidance, and a knowledge transfer session

Remediation unlocks secure, compliant, and resilient Intune device



Who should be interested

The engagement is intended for security decision-makers such as:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- Endpoint & Device Management owners/ decision makers
- Application business owners
- IT Security
- IT Operations
- Security Architect
- Security Engineers

Why TechNet UC?

When it comes to unified endpoint management you need an experienced partner.

We have helped hundreds of customers. Let us help you too.

TechNet UC

 | www.technetuc.com | info@technetuc.com | (984) 777-5645